The Legal Side of IoT Cloud Systems

Szilvia Varadi* and Attila Kertesz†
* Department of European and International Law, University of Szeged, Hungary
† Software Engineering Department, University of Szeged, Hungary
Email: varadiszilvia@juris.u-szeged.hu, keratt@inf.u-szeged.hu

I. Introduction

As a growing number of communicating devices join the Internet, we will soon face a foggy and cloudy world of interconnected smart devices. Cloud systems already started to dominate the Internet, with the appearance of things of the Internet of Things (IoT) area IoT Cloud systems are formed that still needs a significant amount of research. IoT is a rapidly emerging concept where sensors, actuators and smart devices are often connected to cloud systems. Clouds are used in scenarios in which data from a large set of sensors is processed and often fed back to actuators or smart devices. The Cluster of European Research Projects on the Internet of Things [1] defined the Internet of Things (IoT) as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols. Things in this network interact and communicate among themselves and with the environment by exchanging data and information sensed, and react autonomously to events and influence them by triggering actions with or without direct human intervention.

According to recent Gartner reports [2], there will be 30 billion devices always online and more than 200 billion devices discontinuously online by 2020. Recent trends and estimations call for an ecosystem that provides means to interconnect and control these devices. With the help of cloud solutions, user data can be stored in a remote location, and can be accessed from anywhere. Legal and regulative constraints increase the complexity further and vary depending on the location of different stakeholders. In the supply of any goods and services, the law gives certain rights that protect the consumer and provider, which also applies for IoT cloud systems: it is subject to legal requirements and constraints to ensure cloud services are accurately described and provided to customers with guarantees on quality and fitness-for-purpose.

Data that users produce with mobile devices are continuously posted to online services, which require the use of cloud providers to efficiently handle these data. In this paper we address the legal side of these systems. In our previous work we have derived a general federation architecture for clouds from definitions of international organizations, and used it to define common cloud computing usage patterns [3]. The aim of this work is to broaden this investigation for cases involving IoT utilization. Once the new rules set out in the General Data Protection Regulation (GDPR) of EU [5] is clarified, we plan to map these the legal constraints to IoT Cloud use cases, in order to help users to better understand the ecosystem and companies to design better applications for IoT cloud systems.

The remainder of this paper is as follows: Section II summarizes earlier identified cloud use cases and their legal aspects. Section III introduces general IoT application areas and discusses recent advances in European legislation and their implied regulative constraints to IoT Cloud systems. Finally, we conclude the paper in Section IV.

II. Legal Constraints of Cloud Use Cases

As a result of the pace of technical and economic progress in clouds, it was important to determine the compliance of common cloud computing usage patterns with legal constraints and requirements. To protect the consumer against the provider misusing their data, data processing legislation has been developed to ensure that the fundamental right to privacy is maintained. Data protection covers the dynamic provisioning and processing of data in cloud environments including the majority of currently available cloud characteristics and functions (e.g., shared data storages, multi-jurisdictional servers and establishments). The distributed nature of cloud computing (i.e. cloud services being available from anywhere in the world) makes is difficult to analyze every country's data protection laws for common cloud usage evaluation criteria. Therefore it is important to know how the corresponding legislation affects the behavior of cloud providers.

In a former work [3] we provided a method for and the results of an evaluation of commonly-observed cloud federation use cases against the law applied to cloud computing. To clarify and exemplify legal compliance in the identified usage patterns, we considered the Data Protection Directive (DPD) of the European Union [4] from 1995, which is a commonly accepted and influential directive in the field of data processing legislation. We discussed where legal issues may arise due to private data processing at multiple jurisdictions resulting from utilizing cloud data center establishments at different geographical locations. Considering European cloud federations, the Article 4 of the current DPD states that the location of the data controller's establishment determines the national law applicable for data processing. In cases where an establishment is outside the EU, an adequate level of data protection should be provided according to the DPD.

III. New European Regulation for IoT Cloud Environments

IoT application areas and scenarios have been categorized, such as by Want et al. [6], who set up three categories: (i) Composable systems – ad-hoc systems can be built from a variety of nearby things by making connections among these possibly different kinds of devices. As these devices can discover each other over local wireless connections, they can be combined to provide higher-level capabilities. (ii) Smart cities – utilities of modern cities could be managed more efficiently with IoT technologies, e.g. traffic-light systems can be capable of sensing the location and density of cars in the area, and optimizing red and green lights to offer the best possible service for drivers and pedestrians. (iii) Resource conservation – with the extensive use of Internet-connected, networked sensors major improvements can be made in the monitoring and optimization of resources such as electricity and water.

The European Commission is currently in the last phase of reforming the European data protection rules, where the main objectives are: to modernize the EU legal system for the protection of personal data to respond to the use of new technologies; to strengthen users' influence on their personal data and to reduce administrative formalities; and to improve the clarity and coherence of the EU rules for personal data protection. To achieve these goals, the Commission created a new legislative proposal, called General Data Protection Regulation (GDPR) [5], a regulation that sets out a general EU framework for data protection to replace the currently effective DPD. In IoT Cloud systems, personal data is increasingly being transferred possibly across borders and stored on servers in multiple countries both within and outside the EU. The globalised nature of dataflows calls for strengthening the individuals' data-protection rights internationally. This requires strong principles for protecting individuals' data, aimed at easing the flow of personal data across borders while still ensuring a high and consistent level of protection without loopholes or unnecessary complexity. In these legal documents the Commission aims to introduce a single set of rules on data protection. It places increased responsibility and accountability for the companies processing personal data (e.g. they must notify the national supervisory authority of serious data breaches within 24 hours). It promotes a single national data protection authority in each EU country that people can refer to, even when their data is processed by a company based outside the EU. These authorities will be empowered to fine companies that violate EU data protection rules. It strengthens the right to data portability by enabling easier access to users' personal data, and easier data migration among service providers. It introduces the "right to be forgotten" to enable the deletion of user data upon request, when there are no legitimate grounds for retaining it. Some providers claim in the service usage terms and conditions to have the right to retain data, which may be affected by this new regulation. Finally, it explicitly states that EU rules must be applied for data processing outside the EU by companies that are active in the EU market.

As a summary, due to the legal nature of a regulation under EU law, the proposed data protection Regulation will establish a single rule that applies directly and uniformly. Considering IoT Cloud use cases: according to the Article 4 of the current DPD, the location of the data controller's establishment determines the national law applicable, which can be variable as we have seen in the use cases mentioned in our previous work [3]. However, the proposed Regulation with its unified rules after coming into force (planned in 2018) must be applied in every Member State in the same way, so there would be and could be not discrepancy among them. Moreover where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the EU, such as in a Member State's diplomatic mission or consular post (Preamble (22) of [5]).

IV. Conclusions

In this paper we introduced that the Internet of Things is a rapidly emerging concept where sensors, actuators and smart devices are often connected to the Cloud forming IoT Cloud systems. We discussed that the European Union has already taken steps to reform its data protection legislation with the new General Data Protection Regulation that aims to establish a single rule that applies directly and uniformly in Europe. With this work we only started to examine this legal novelty to be applied for IoT Clouds, and our future work plans to map these these legal constraints to specific IoT Cloud use cases, to help users to better understand this ecosystem and to design better applications.

Acknowledgements

The research leading to these results was supported by the UNKP-UNKP-16-4 New National Excellence Program of the Ministry of Human Capacities of Hungary.

References

[1] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelffle. Vision and Challenges for Realising the Internet of Things. CERP IoT - Cluster of European Research Projects on the Internet of Things, CN: KK-31-10-323-EN-C, March 2010.

[2] J. Mahoney and H. LeHong, The Internet of Things is Coming, Gartner report. Online: https://www.gartner.com/doc/1799626/internet-things-coming, Sept. 2011.

[3] A. Kertesz, Sz. Varadi, Legal Aspects of Data Protection in Cloud Federations. In S. Nepal & M. Pathan (Ed.), Security, Privacy and Trust in Cloud Systems, pp. 433–455, Berlin, Heidelberg. Springer-Verlag, 2014.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, pp. 31–50, 1995.

[5] COM (2012) 11 final, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, Jan. 2012.

[6] R. Want, S. Dustdar, Activating the Internet of Things. Computer, Vol. 48, No. 9, pp. 16–20, 2015.